令和元年度情報セキュリティ等監査結果

「校務処理システム」における情報セキュリティについて　　対象受検機関：教育庁教育振興室高等学校課

<table>
<tr><th>事務事業の概要</th><th>検出事項</th><th>改善を求める事項（意見）</th></tr>
<tr>
<td>１　対象システムの概要
　校務処理業務については、旧来は各府立学校が独自に構築したシステムにより利用されていたが、事務の負担軽減を図るため高等学校課により全府立学校共通のシステムとして導入された。
　主な機能として、校務処理に係る生徒の個人情報を登録、参照する機能が提供されている。
　現在の校務処理システムは、府立学校の職員が校務で利用する専用ネットワークである「統合ICTネットワーク」内で運用されている。統合ICTネットワークは高等学校課により運用されており、各府立学校は高等学校課から配布されたパソコンを利用してアクセスすることができる。また、統合ICTネットワークでは校務処理システムの他、インターネット、メール、ファイルサーバ等の機能も提供される。
　校務処理システムに係る情報資産については、重要度に応じた分類が教育庁より各府立学校へ通達されており、各府立学校はこの通達と「教育委員会セキュリティポリシー実施手順」（以下「セキュリティポリシー」という。）に基づき情報資産の分類及び管理ルールを定めて運用を行っている。
　最も重要度の高い「重要度Ⅰ」の紙媒体等による情報資産については、施錠保管、持出禁止、廃棄時の裁断処理、「重要度Ⅱ」の情報資産については、やむを得ず持ち出す場合の承認、廃棄時の裁断処理等のルールを定めて管理を行っていた。

≪情報資産の重要度と主なデータ≫
<table>
<tr><th>重要度</th><th>内容※１</th><th>例※２</th></tr>
<tr><td>Ⅰ</td><td>・情報が脅威にさらされた場合に実害を受ける危険性が高い情報
・システム設定や個人情報等の秘匿情報</td><td>・指導要録
・出席簿
・生徒指導カード
・成績に関する個票
・健康診断に関する個人情報</td></tr>
<tr><td>Ⅱ</td><td>・情報が脅威にさらされた場合に実害を受ける危険性は低いが重要性が高く、公開することを予定していない情報</td><td>・生徒名簿、住所録
・緊急連絡先
・通知表
・保健室来室に係る記録</td></tr>
<tr><td>Ⅲ</td><td>・上記以外の情報</td><td>・生徒指導計画
・授業用教材</td></tr>
</table>
※１：「教育委員会情報セキュリティセキュリティポリシー実施手順」より
※２：「教育委員会情報セキュリティセキュリティポリシー実施手順の運用」より</td>
<td>１　重要性に応じた情報資産の分類と管理
　情報資産の重要度に応じた分類が教育庁より各府立学校へ通達されており、各府立学校はこの通達とセキュリティポリシーに基づき情報資産の分類及び管理ルールを定めて運用しているところであるが、持ち出し禁止とされている生徒指導カードを家庭訪問時に持ち出していた。

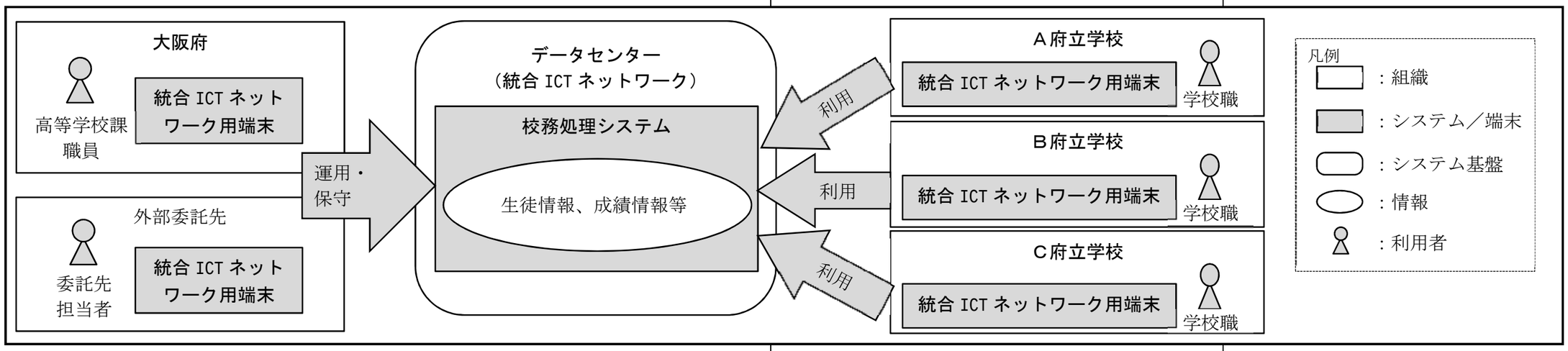
２　ユーザＩＤの設定と権限管理について
　校務処理システムのユーザＩＤについては、各府立学校で管理しており人事異動の際に追加や削除を行っている。なお、ユーザＩＤは、「システム管理者」、「学校管理者」、「学年主任」、「一般職員」とそれぞれの職責に応じて権限の付与ができるが、一部の学校において本来の職責以上の権限があるユーザＩＤが付与されていた。また、「校務処理システムの適正管理について」（平成28年４月15日付け教育振興室長通知）（以下「室長通知」という。）により原則利用禁止とされている共用ＩＤが利用されており、自身のユーザＩＤでは閲覧できない情報について、閲覧できるようになっていた。さらには、共用ＩＤのパスワードは、定期的な変更がされていなかった。

３　操作ログの監視について
　室長通知では、操作ログの定期的な監視を求めているが、実地監査をした２校において操作ログの監視は行われておらず、室長通知の存在についても把握されていなかった。</td>
<td>１　管理ルールに従った運用がされていない場合、紛失や盗難等による情報漏えいのリスクがあることから、通達及びセキュリティポリシーについて、情報利用の必要性と情報の適正な管理の確保を勘案した具体的なルールを検討するとともに、厳格に運用すること。

２　職責以上の権限が付与された場合、不正なＩＤの追加など不正アクセス等を招くおそれがあることから、必要最小限の権限を割り当てることを検討すること。また、共用ＩＤについては、権限がオールマイティで、恣意的に運用されると情報管理に著しい支障をきたすおそれがあることから廃止すること。

３　操作ログの定期的な監視が実施されていない場合、不正アクセス及び不正操作がされていても検知が遅れることが考えられる。今回、２校の実地監査をしたところでは、操作ログ確認はされておらず、また、室長通知の認識もなかったことから、改めて操作ログの監視の必要性及び監視方法等を各府立学校長に対し周知徹底をするとともに定期的に高等学校課において操作ログの確認について指導を行われたい。</td>
</tr>
</table>

≪情報システムの運用・利用イメージ≫



2　監査における着眼点

No	着眼点	S.No	内容（詳細）
1	情報資産の分類と管理	(1)	重要な情報資産が不適切に取扱われないよう、情報資産が重要度に応じて分類され、適切に取扱われているか
2	情報システム全体の強靭性の向上	(1)	ネットワーク経由のシステムへの不正侵入を防止するための対策が講じられているか
3	物理的セキュリティ	(1)	サーバ、パソコン等の機器が、盗難や損傷等の物理的被害から保護されているか
4	人的セキュリティ	(1)	重要な情報の保護、パソコン等機器の適正な取扱い等の、情報セキュリティに関する研修や教育が適時に行われているか
5	技術的セキュリティ	(1)	パソコン及び電磁的記録媒体について、不正な情報の持ち出し等を防止するための対策が講じられているか
		(2)	ユーザ ID、パスワード及び権限の不正利用を防止するための対策が講じられているか
		(3)	ウイルス感染からシステムを保護するための対策が講じられているか
		(4)	脆弱性を利用した攻撃からシステムを保護するため、ソフトウェアの脆弱性情報を収集し、適時にパッチの適用を行っているか
		(5)	システムへの不正アクセス等を速やかに発見するため、セキュリティに関するログの保管、分析が行われているか
6	運用	(1)	セキュリティに関する事故が発生した場合の報告先が定められ、速やかに報告が行われているか
7	外部サービスの利用	(1)	外部委託先においてセキュリティ対策が適切に実施されるよう、外部委託先を適切に監督しているか

3　実施方法と確認方法

事前ヒアリングにより事業の概要等を調査した上で、質問表を作成し、情報セキュリティ関連文書の閲覧及び監査対象機関への実地監査により回答を求めた。

また、システム操作等については、サンプルとして２校を選定し実機確認をした。

監査（検査）実施年月日（委員：ー年ー月ー日、事務局：令和元年８月８日から同年12月10日まで）